E-Embargoes: Discouraging Traffic Manipulation With Incentives

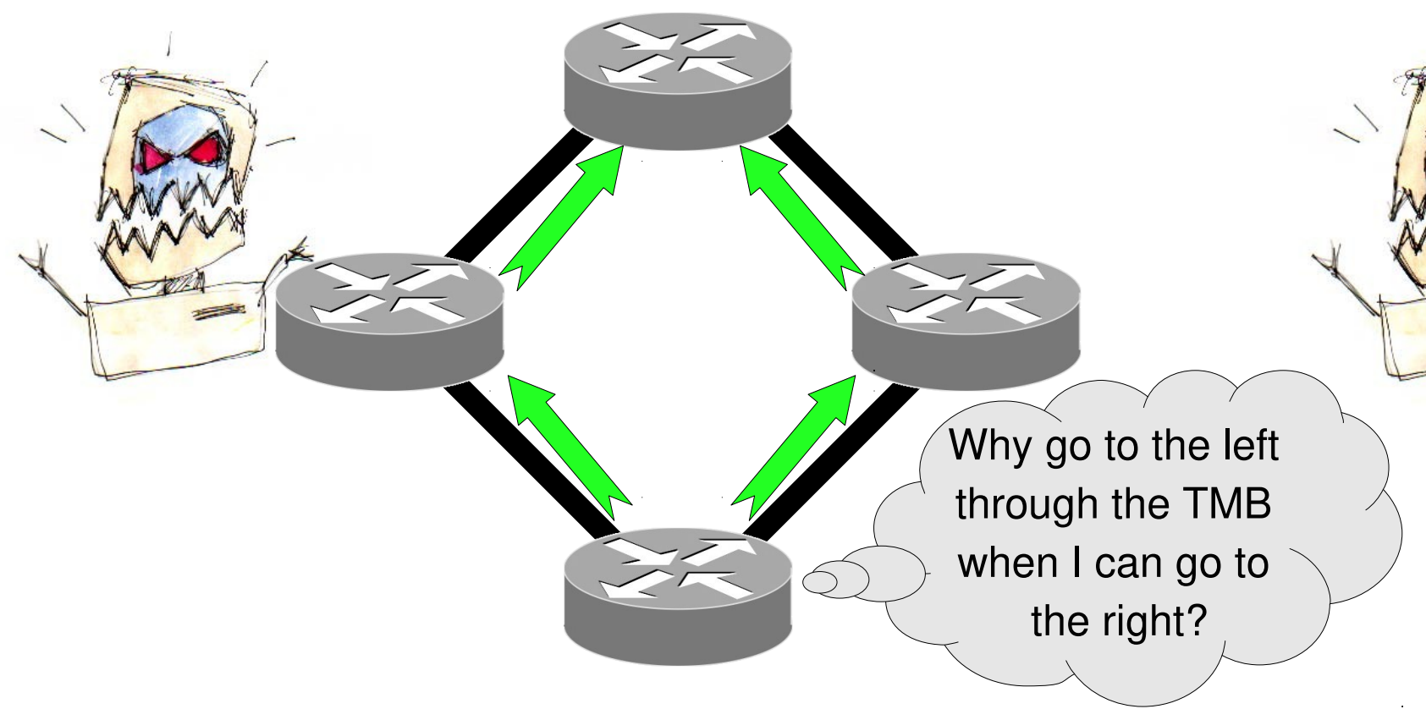
Max Schuchard and Nicholas Hopper
University of Minnesota

Abstract

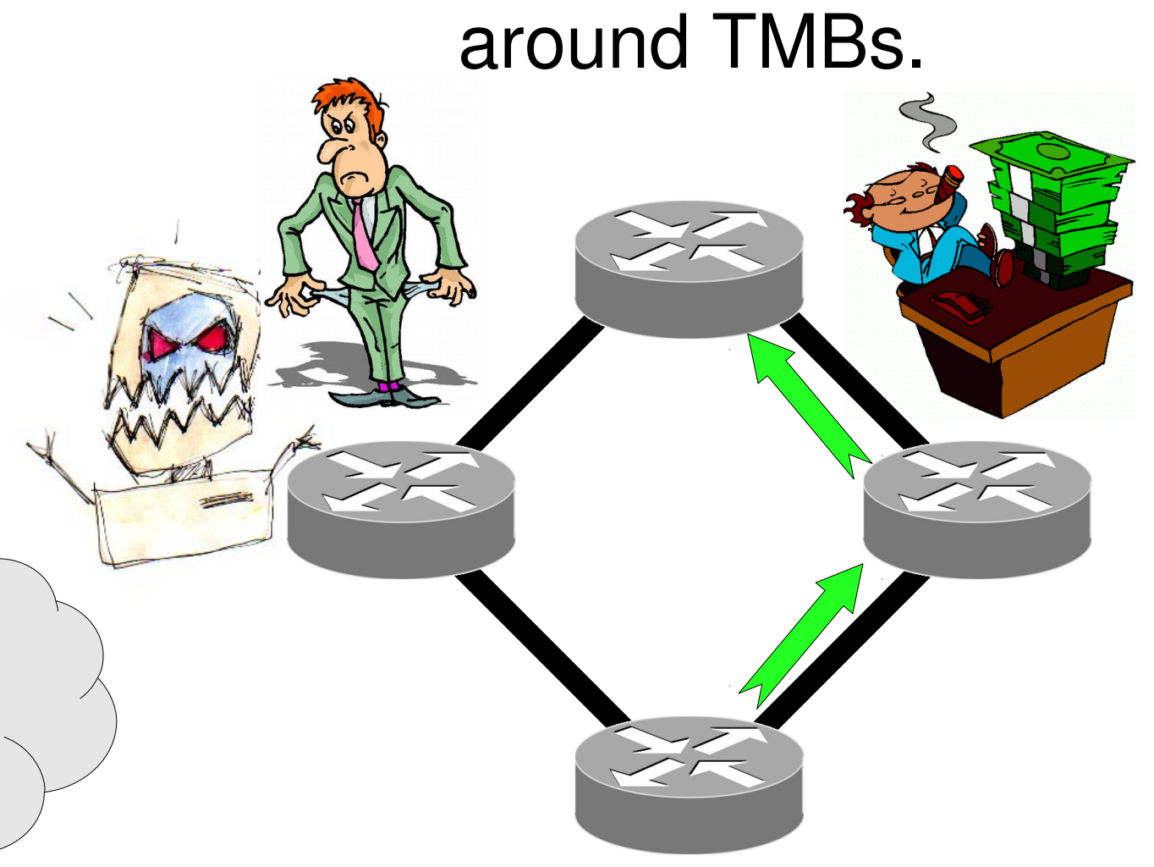
- Systems exist which take advantage of privileged position in the transit core of the Internet to observe and manipulate traffic in flight
  - We term these *Traffic Manipulating Boxes (TMBs)*
  - Transit ASes which host these we call *Deployers*
- *Routing Capable Adversaries* can directly attack the availability of such systems by routing around TMBs
- **We examine how Routing Capable Adversaries are also powerful *economic* adversaries**
  - Our Routing Capable Adversaries, called *resistors*, inflict economic losses on deployers via reduced transit revenue, incentivizing TMB removal

Routing Capable Adversaries & the Movement of Cash on the Internet

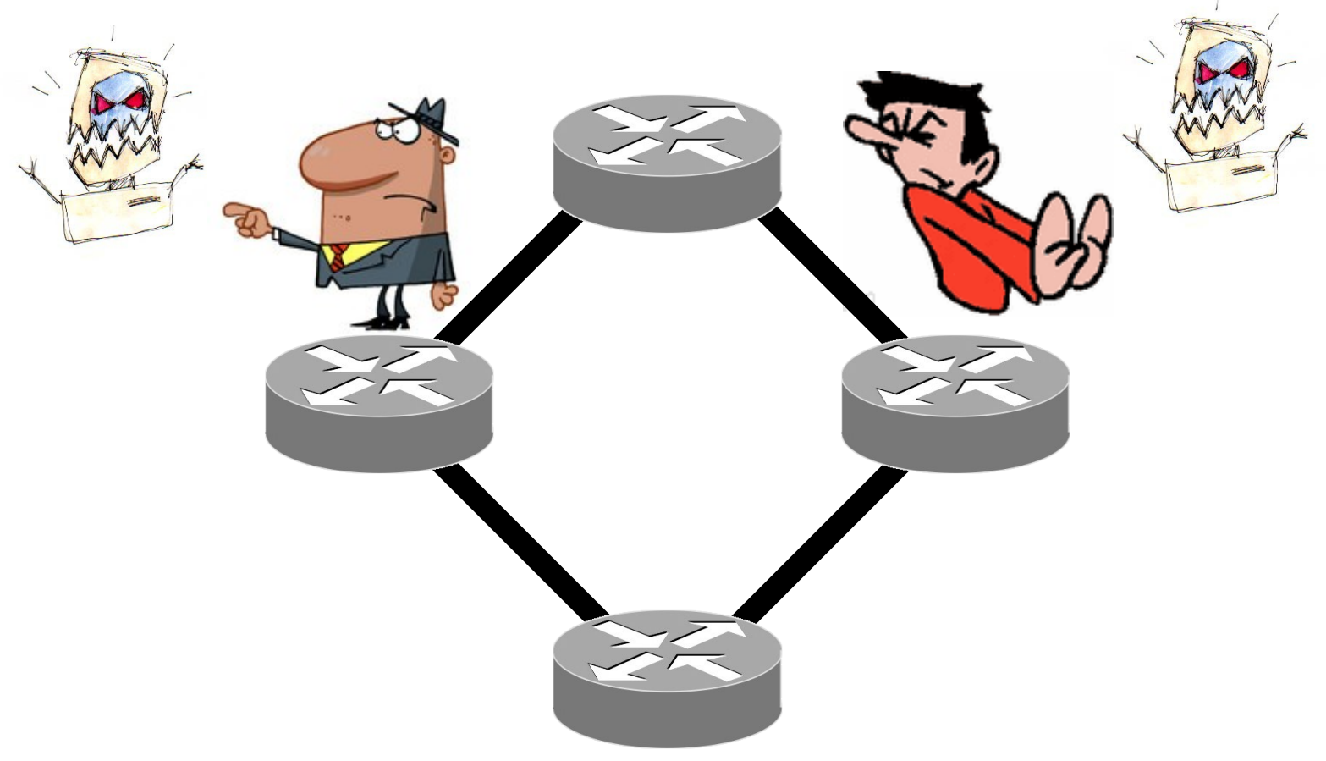
Routing capable adversaries can alter the BGP decision making process, preferentially selecting routes avoiding TMBs.


Why go to the left through the TMB when I can go to the right?

Deployer ASes lose transit revenue when resistors route around TMBs.



Deployer ASes are incentivized to remove TMBs, non-deployers are incentivized to not install TMBs.



Routing Capable Adversary Strategies & Resistor Costs

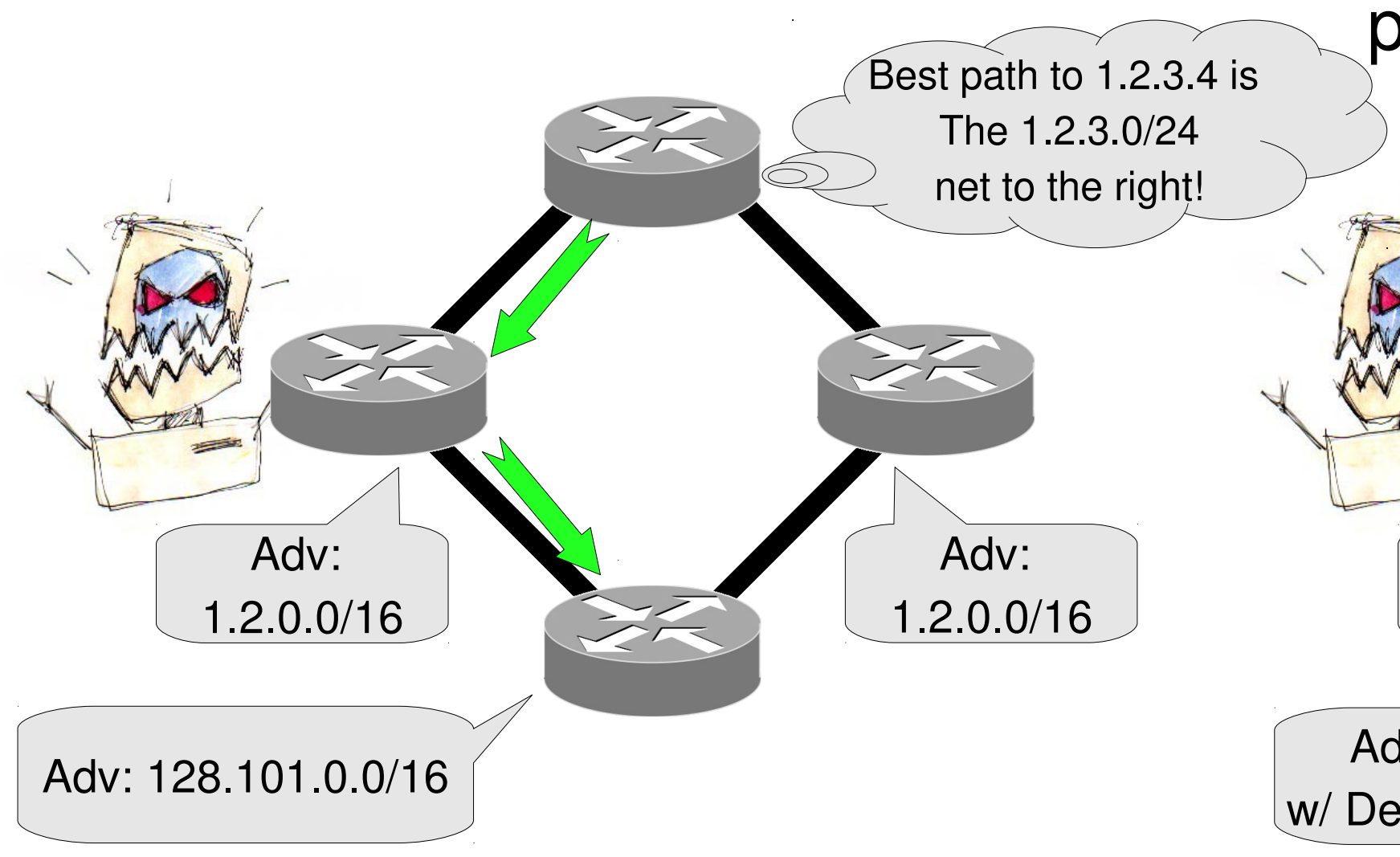
Resistor Type	Transit Conversion	Increased Transit Costs	Reduced QoS
Original RAD	Yes	Yes	Yes
Local Pref	No	Yes	Yes
Path Length	No	No	Yes
Tiebreak	No	No	No

Impacting Incoming Traffic

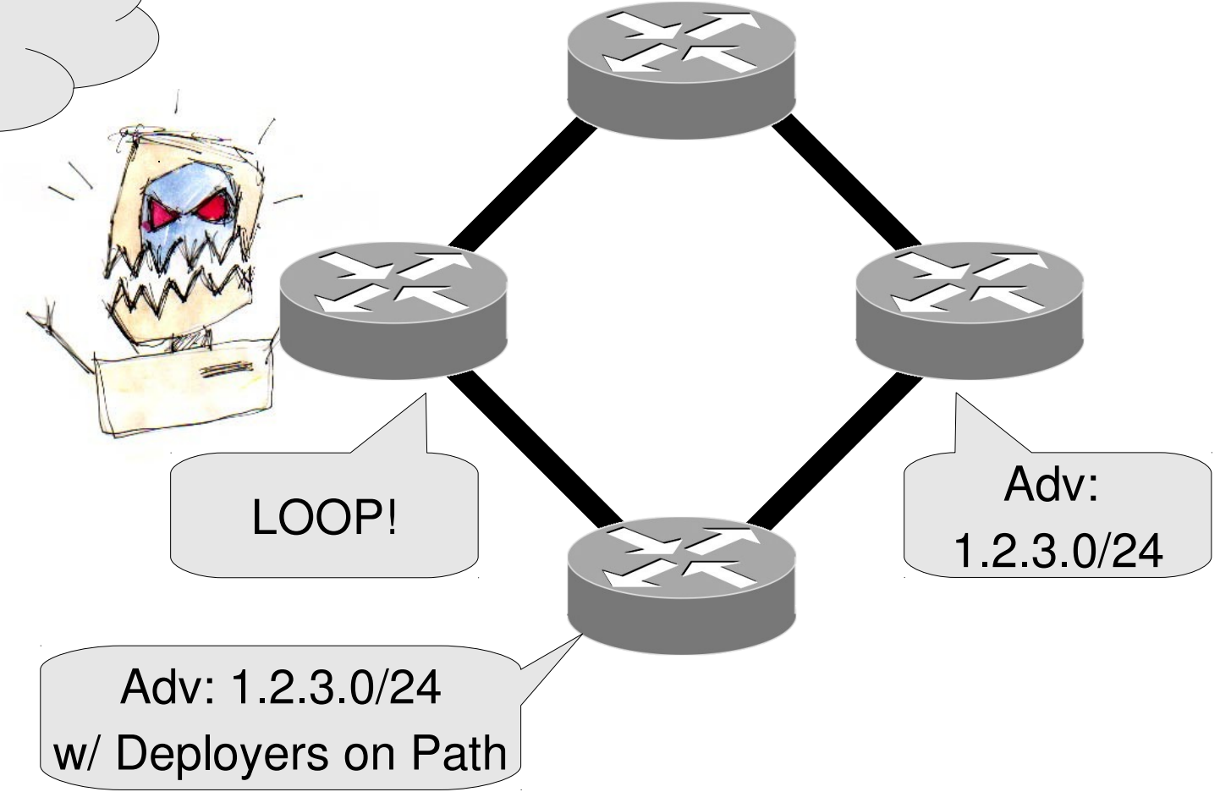
- Path selection decisions only control ***outbound*** traffic, not ***inbound***
- ***Fraudulent Route Reverse Poisoning*** (FRRP) uses BGP hole punching to reroute incoming traffic
  - BGP allows for sub-blocks of existing IP blocks to be advertised
  - Packets are forwarded along the best path to the *most specific* prefix known
  - Resistors can falsely add all deployer ASes to the BGP path of advertised routes
  - Deployers will ignore these routes because of loop detection, and not propagate them

Fraudulent Route Reverse Poisoning

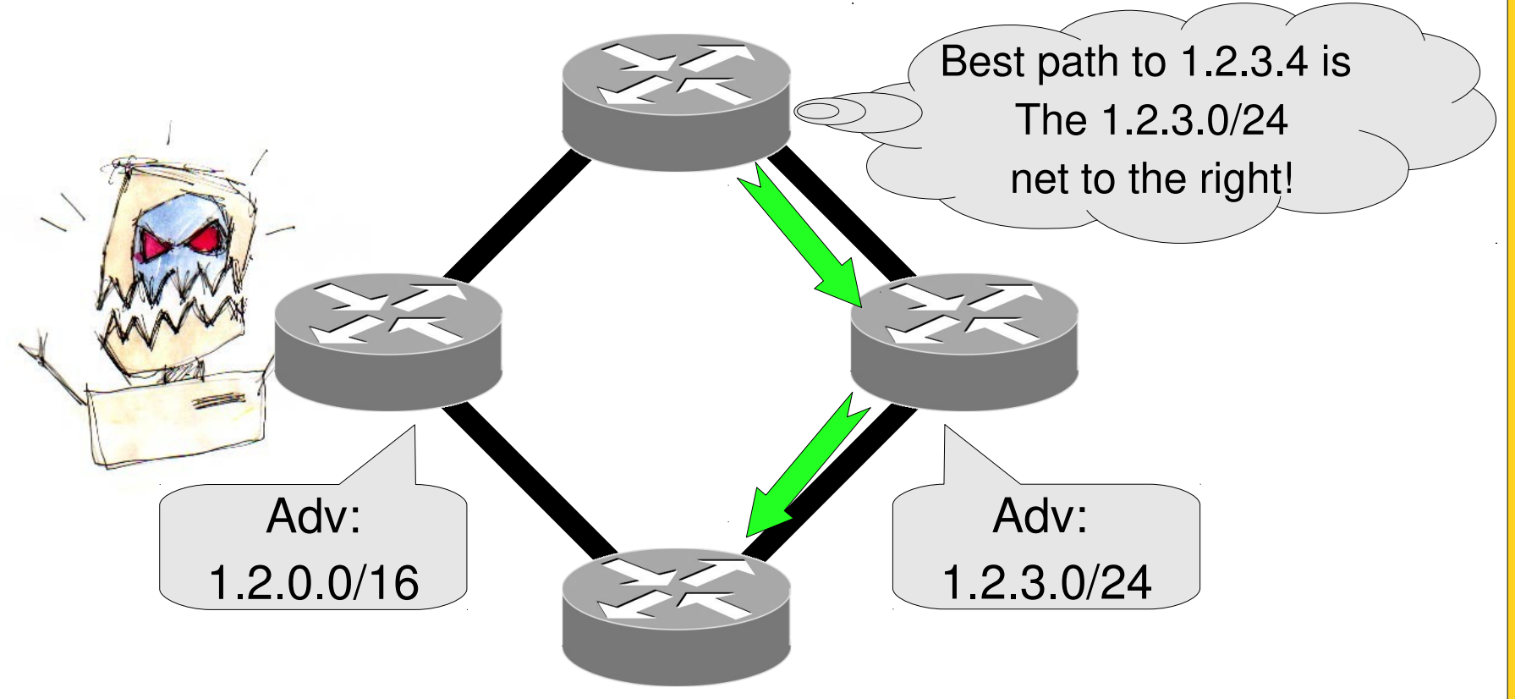
Non-resistors will send traffic bound to resistors across TMBs.



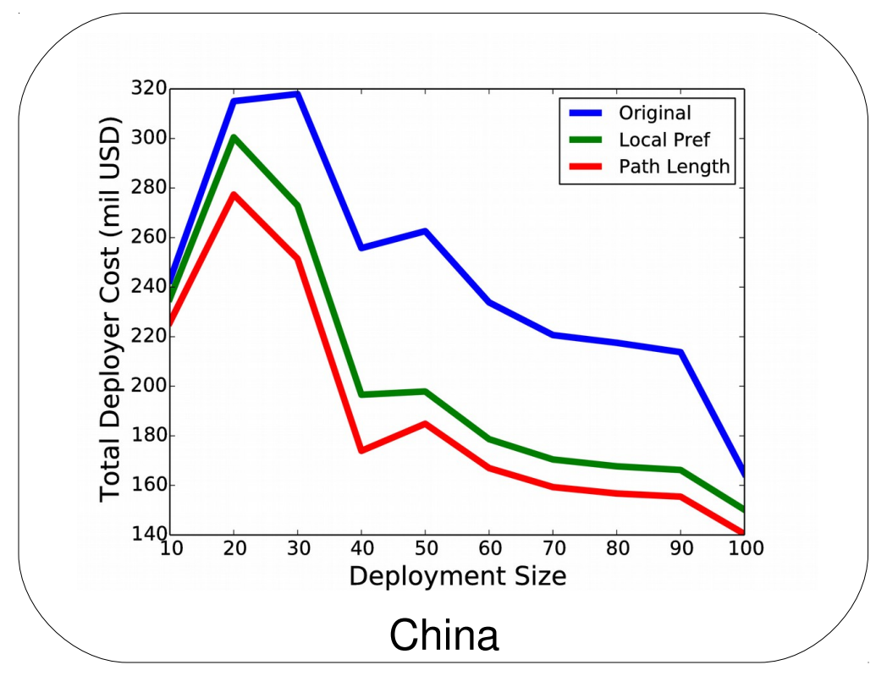
Resistors hole punch routes adding deployers to the path, preventing deployer propagation.



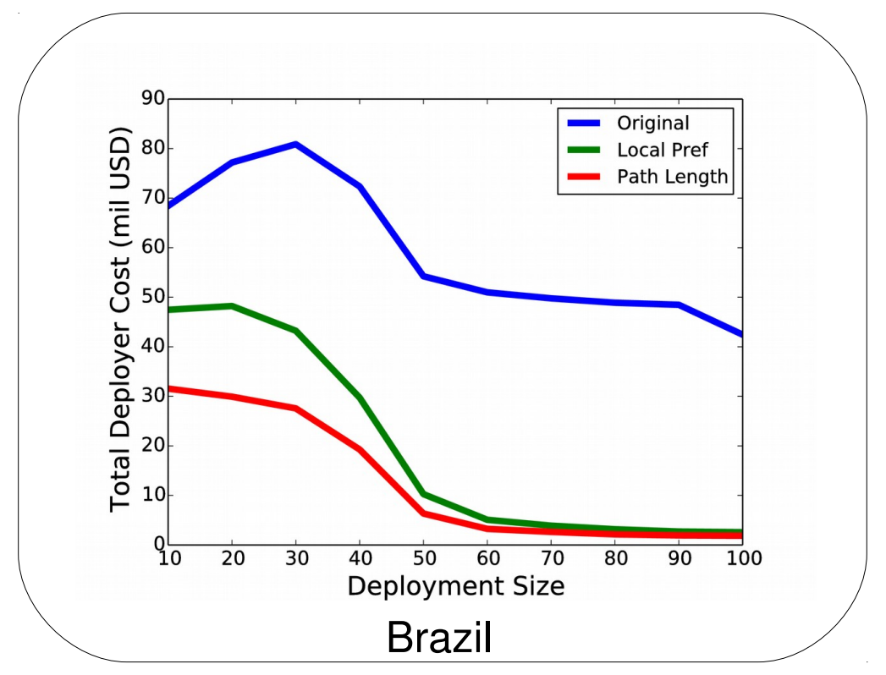
BGP will forward based on most specific prefix, which deployers could not propagate.



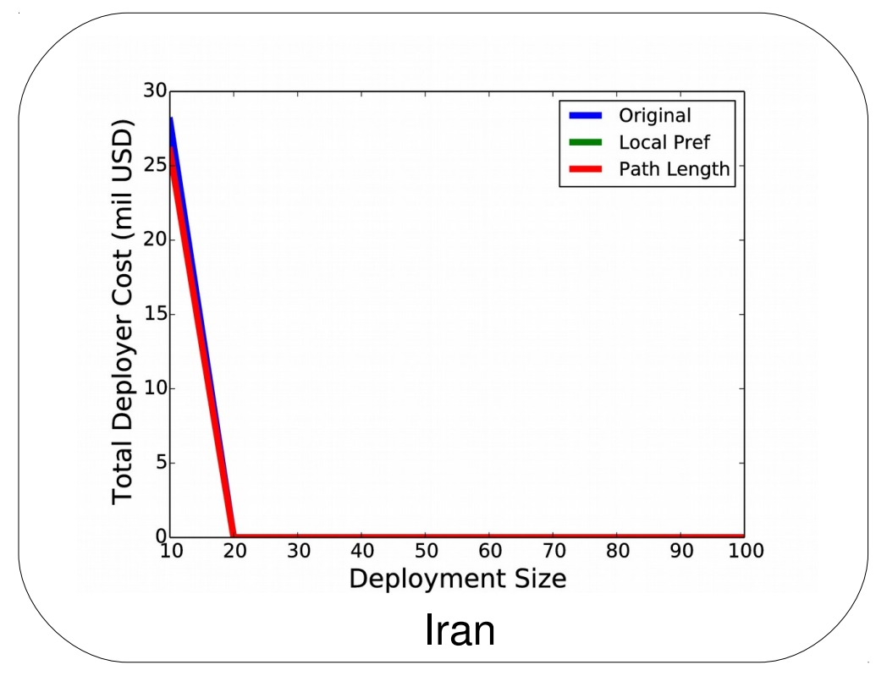
Annual Direct Revenue Losses



China



Brazil



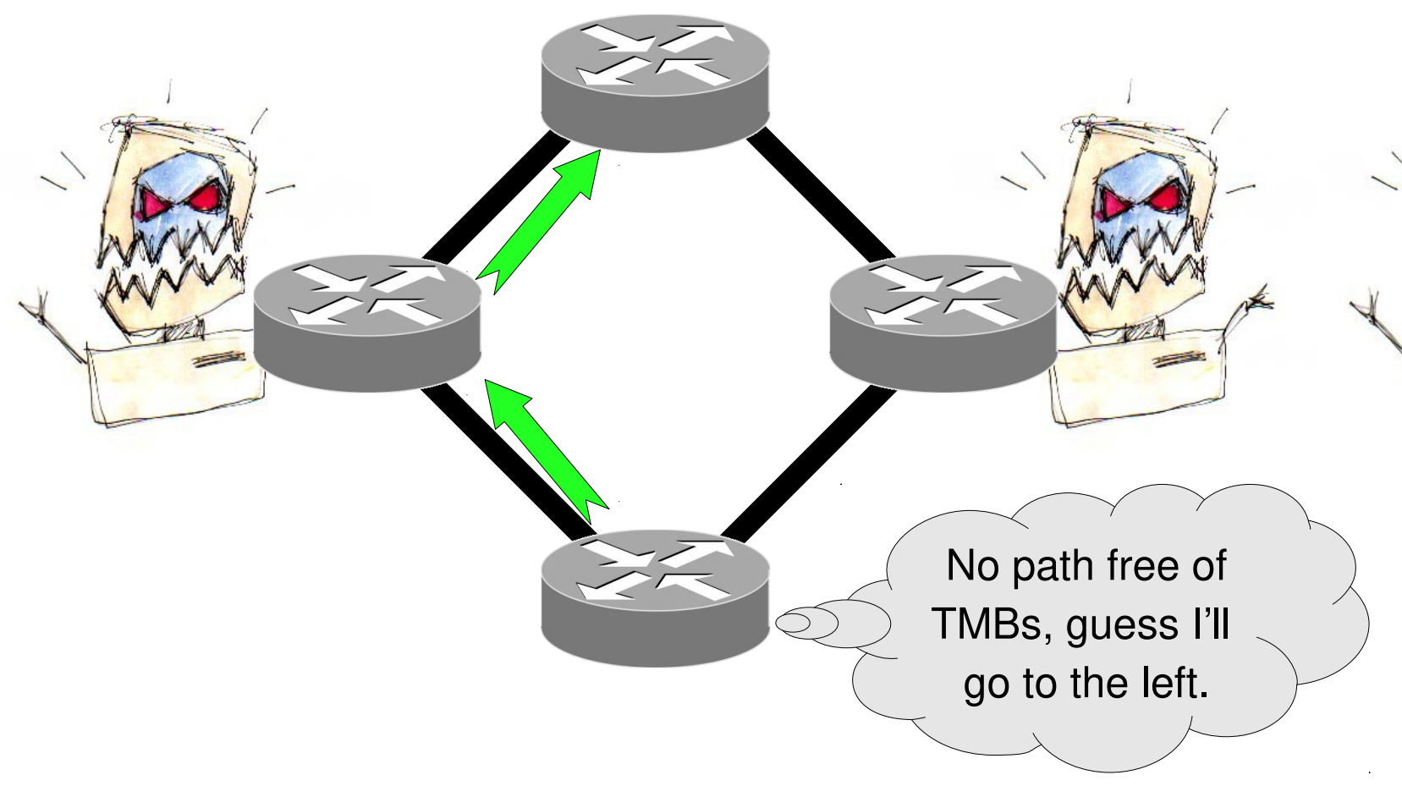
Iran

Deployer Opportunity Costs

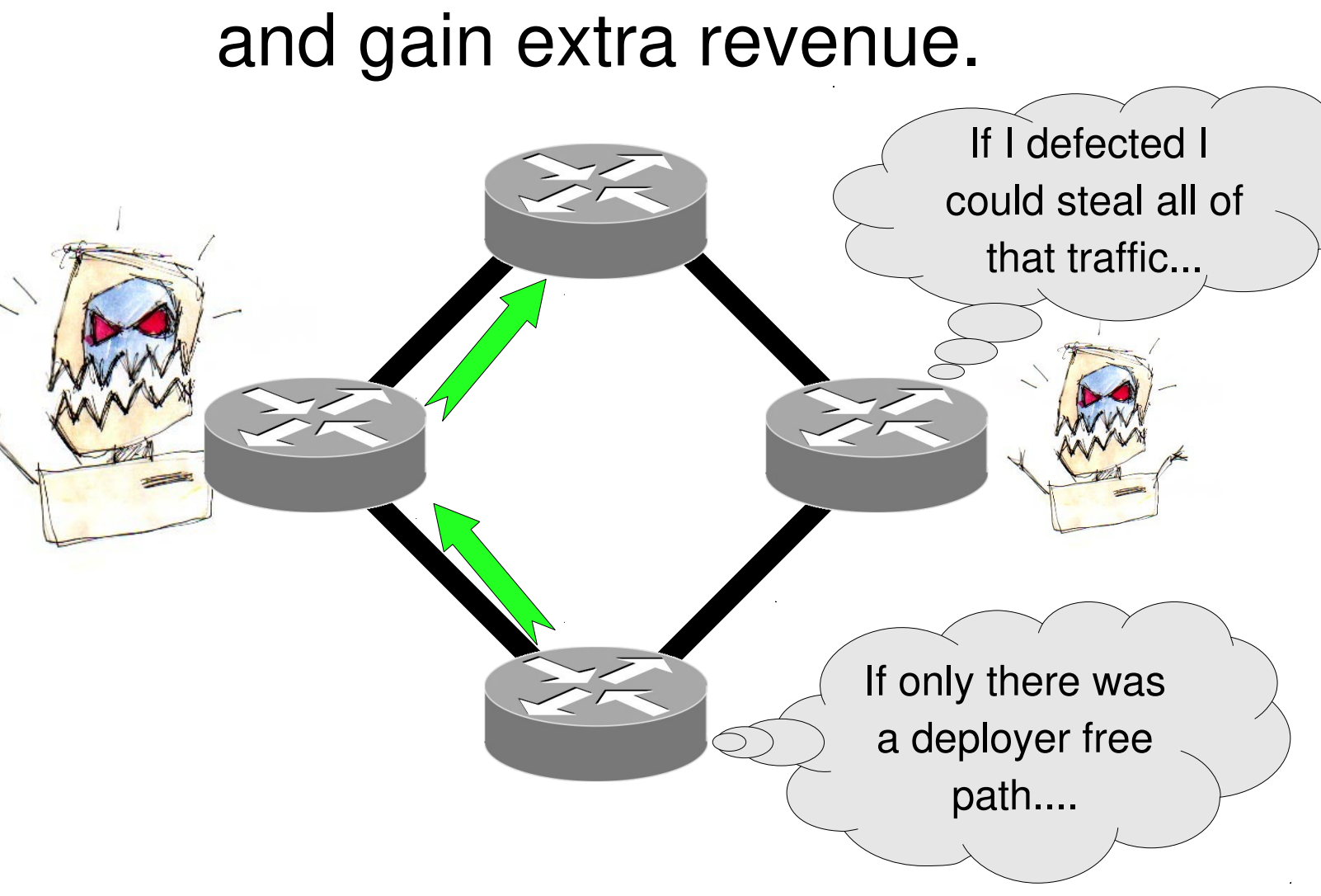
- Deployers see additional opportunity costs when there are destinations ***only*** reachable via deployers
- One deployer will be the best (i.e. utilized) AS
- If a non-utilized deployer removes TMBs they would be preferentially selected as the best path
  - Steals traffic from other deployer ASes
  - This is in ***addition*** to traffic they had lost to non-deployers, which is also recovered via defection
- These opportunity costs we call ***Defection Costs***
- Unlike direct costs, these *increase* as the number of deployers increases

Deployer Defection

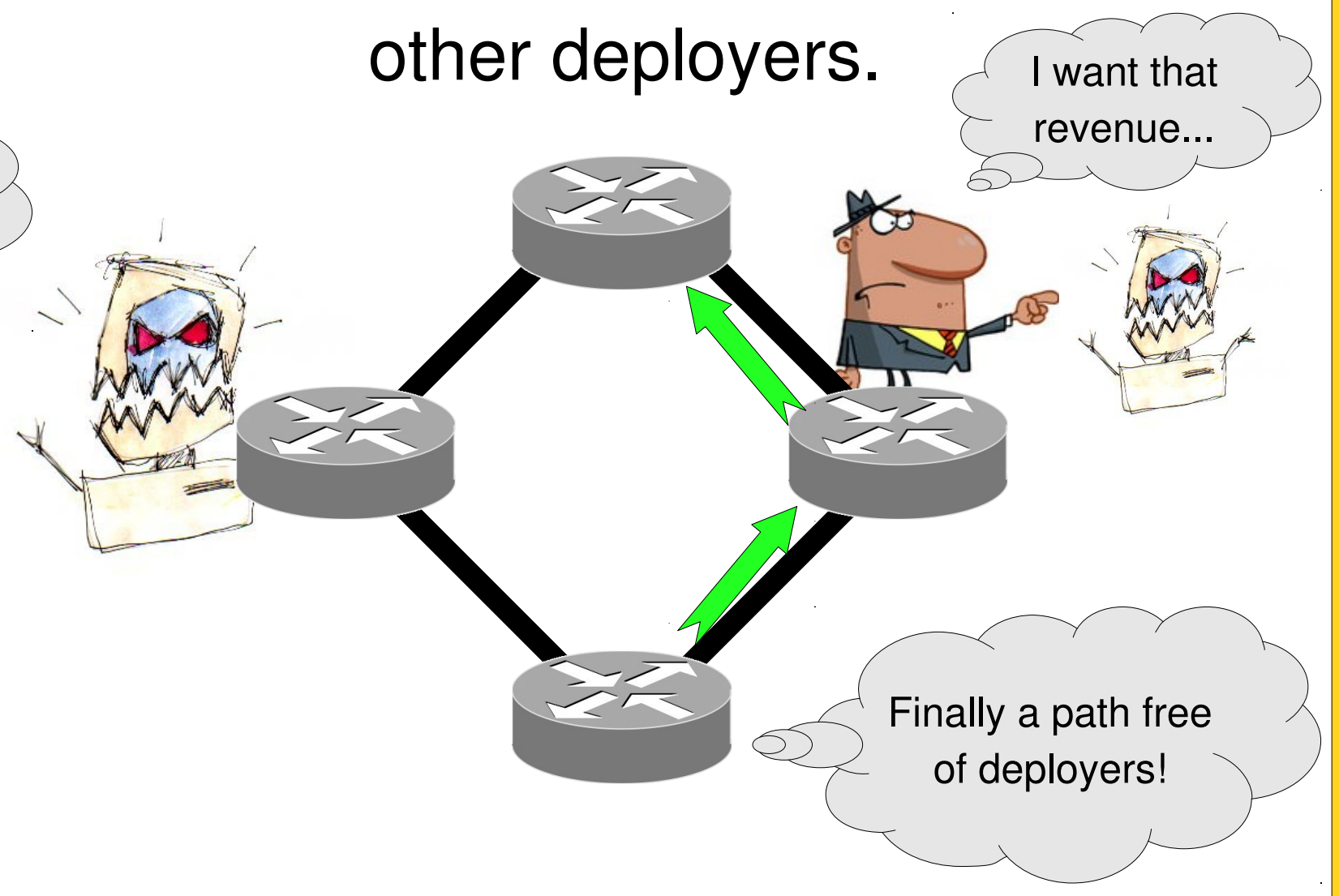
If there is no path to a destination free of TMBs, resistors must send traffic via a deployer.



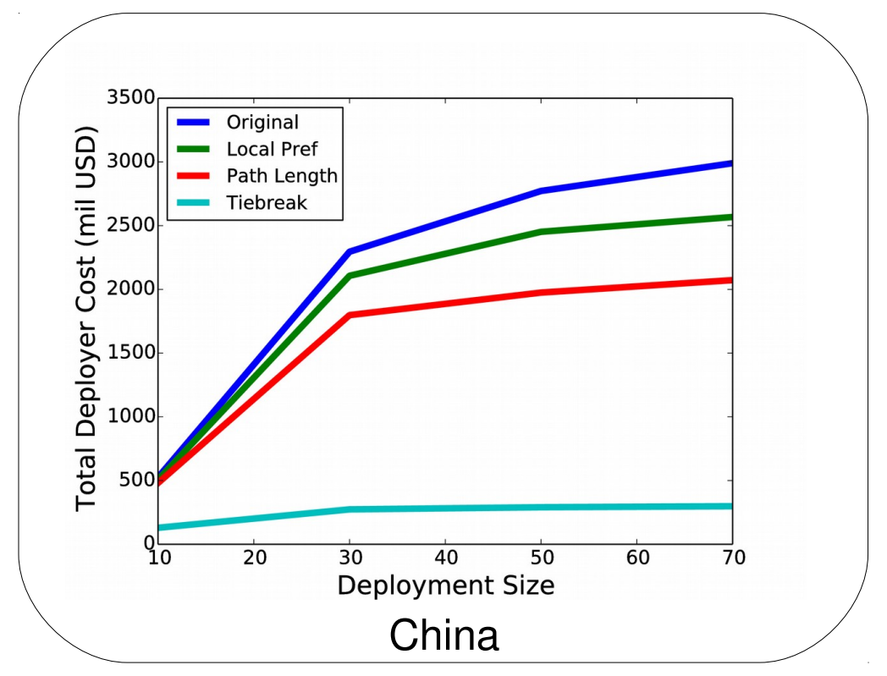
If a deployer defects, it would automatically be the best path and gain extra revenue.


If I defected I could steal all of that traffic...
If only there was a deployer free path....

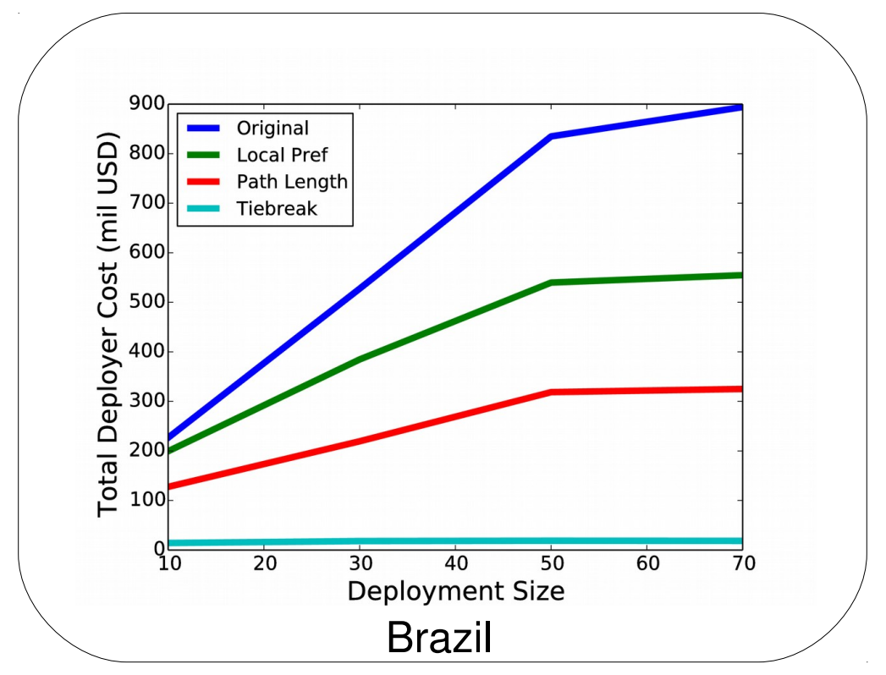
Deployers are incentivized to defect to steal away traffic from other deployers.



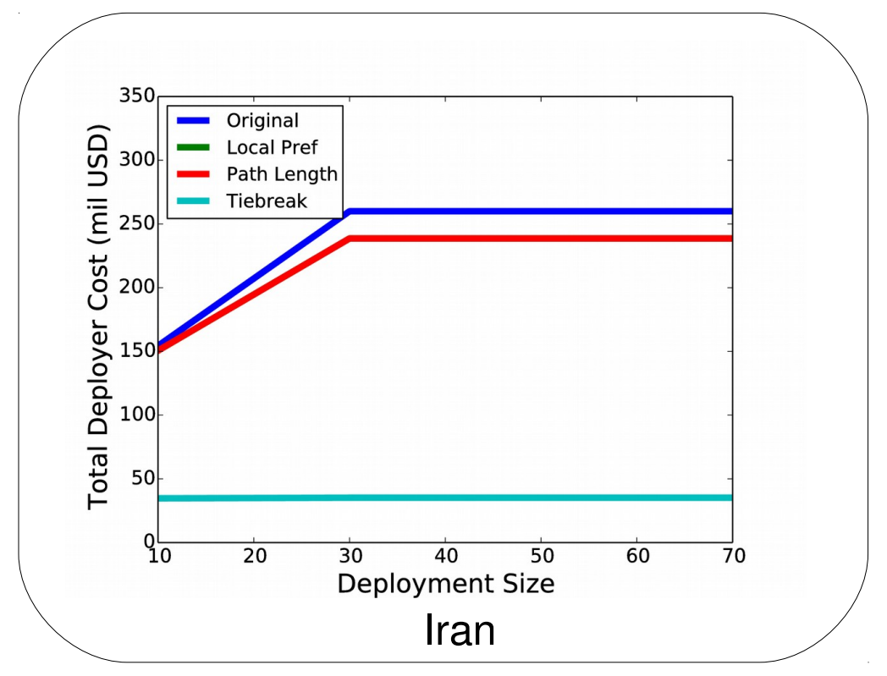
Annual Losses With Defection Costs



China



Brazil



Iran